UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

ENARGY POWER CO. LTD. et al.,	)	
Plaintiffs	)	
v.	)	**Civil Action No. 13-11348-DJC**
XIAOLONG WANG et al.,	)	
Defendants.	)	

STATEMENT OF REASONS

CASPER, J. **December 3, 2013**

I. Introduction

Plaintiffs Energy Power Co. Ltd. ("Enargy"), Enargy Corporation, Jacky Chen ("Jacky Chen") and Zoomkoh Management LLC (collectively "Plaintiffs") have moved for a preliminary injunction: (1) compelling Defendant Xiaolong Wang ("Wang") to disclose a password for files locked on Enargy's server; (2) requiring Wang to return his copies of these files to Enargy; and (3) ordering Defendant Cecei Chen ("Chen") to cease interfering with a bank account registered to Enargy. D. 7. Plaintiffs also seek an attachment of real property. D. 9. For the following reasons, this motion for a preliminary injunction is ALLOWED IN PART and the motion to attach is DENIED without prejudice.

II. Standard of Review

To obtain a preliminary injunction, the party seeking the injunction must demonstrate: "1) a substantial likelihood of success on the merits; 2) a significant risk of irreparable harm if

the injunction is withheld; 3) a favorable balance of hardships and 4) a fit (or lack of friction) between the injunction and the public interest." Nieves-Marquez v. Puerto Rico, 353 F.3d 108, 120 (1st Cir. 2003). A preliminary injunction is an "extraordinary remedy that may only be awarded upon a clear showing that the plaintiff is entitled to such relief." Winter v. Natural Res. Def. Council, Inc., 555 U.S. 7, 22 (2008) (citing Mazurek v. Armstrong, 520 U.S. 968, 972 (1997)); see also Voice of the Arab World v. MDTV Med. News Now, Inc., 645 F.3d 26, 32 (1st Cir. 2011) (labeling a preliminary injunction as an "extraordinary and drastic remedy") (quoting Munaf v. Geren, 553 U.S. 674, 689-90 (2008)).

III. Factual Background and Procedural History

From February 2008 to August 2011, Wang worked for Enargy as the director of Enargy's research and development department. Affidavit of Jacky Chen, D. 8-1 ¶ 6. As such, Wang led the design and development of a "unique and customized high density DC/DC [power] converter [(the "PH Project")] to be used in specialized aircraft." Id. ¶ 7. Wang worked on the PH Project as well as a similar project called the "Five Series Project." Id. ¶ 11. Together, Enargy and Wang developed a number of trade secrets including "the electric circuit layout, design drawings, bill of material, printing circuit board, software code, structure, experiment data, and testing data." Id. ¶ 8. The parties dispute whether the trade secrets were intended to be the sole property of Enargy or Wang or jointly owned. Id. ¶¶ 8-9; Affidavit of Wang, D. 17-1 ¶ 38. Wang never signed a non-competition agreement with Enargy. Id. ¶ 41.

Over time, the relationship between Enargy and Wang deteriorated. Id. ¶¶ 30-39. By June 2011, Wang was no longer traveling to China to work for Enargy. Id. ¶ 36; D. 8-2 ¶ 8. He stopped working for Enargy in or about August 2011. D. 8-1 ¶ 33. Prior to his departure, Wang, from his home in Canton, Massachusetts, called his assistant in China, Dehua Jiang, and ordered

Jiang to encrypt the PH Project files on Enargy's computer server located in China. Affidavit of Yuning Liu, D. 8-2 ¶ 11. Wang instructed Jiang to condense the files into a single archived file and password protect this file with a "very long password" that Wang read to Jiang over the phone. Id. ¶¶ 12-13. Wang also instructed Jiang to transmit the files to Wang and destroy the original files from Enargy's secure server. Id. ¶ 14. With assistance from Enargy's network administrator, Jiang complied with Wang's orders. Id. ¶¶ 15-18. Enargy has not been able to access the PH Project files since August 2011 and Wang has refused to provide Enargy with the password to the encrypted files on Enargy's server. Id. ¶¶ 19-22. This has made it impossible for Enargy to further develop the product. D. 8-1 ¶ 16. Wang, meanwhile, has continued work on the PH and Five Series Projects with Enargy's distributor-turned-competitor Sichuan Chengye. Id. ¶ 15.

When Wang agreed to work for Enargy, he negotiated a position for his wife, Chen, as treasurer for Enargy's Massachusetts corporation. During her time as treasurer, Chen inserted herself as replacement for Jacky Chen as president of the Massachusetts corporation and removed $330,000 from the corporate bank account. Id. ¶¶ 19-20; D. 8-9; D. 8-11; D. 8-16.

The Court has now heard argument on the pending motions and took the matters under advisement. D. 21.

IV. Discussion

A. Plaintiffs Have Demonstrated a Likelihood of Success on the Merits for Its Claims under the Computer Fraud and Abuse Act and Conversion

"The sine qua non of this four-part inquiry is likelihood of success on the merits: if the moving party cannot demonstrate that [it] is likely to succeed in [its] quest, the remaining factors become matters of idle curiosity." New Comm. Wireless Servs., Inc. v. SprintCom, Inc., 287 F.3d 1, 9 (1st Cir. 2002). Two of Plaintiffs' claims against Wang include an alleged violation of

the Computer Fraud and Abuse Act (Fifth Cause of Action) and Conversion (Seventh Cause of Action). D. 1 at 12-13.

1. Plaintiffs are Likely to Succeed in Their Claim Arising Under the Computer Fraud and Abuse Act

a) The Computer Fraud and Abuse Act

Plaintiffs have alleged that Wang's actions violated the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030. The CFAA criminalizes the unauthorized access of computers under certain circumstances. Id. In addition to the CFAA's criminal application, Congress provided for a private right of action under the statute. 18 U.S.C. § 1030(g) (providing that "[a]ny person who suffers damage or loss by reason of a violation of [the CFAA] may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief"). 18 U.S.C. § 1030(a)(4) provides that:

> Whoever . . . knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $ 5,000 in any 1–year period . . . shall be punished as provided in subsection (c) of this section.

18 U.S.C. § 1030(a)(5)(B), meanwhile, makes it unlawful to "intentionally access a protected computer without authorization, and as a result of such conduct, recklessly cause[] damage." 18 U.S.C. § 1030(a)(5)(B). As Section 1030(a)(4) provides for a finding of liability where the defendant merely "exceeds unauthorized access," the Court evaluates likelihood of success based upon a violation of this provision. Thus, to establish liability under the CFAA, Plaintiffs must demonstrate both that Wang knowingly and with intent to defraud "access[ed] a protected computer" and that his access "exceeded [his] authorized access" and that by means of such conduct furthers the intended fraud and obtained something of value. 18 U.S.C. § 1030(a)(4).

b) Wang's Conduct Constituted "Access"

The parties dispute whether Wang's conduct constituted "access." Plaintiffs contended at oral argument that instructing a third party to access a computer constitutes unauthorized access under the CFAA. Defendants argue that Plaintiffs have not identified a case in which "the CFAA was applied to indirect access of a computer." D. 17 at 12. However, there is nothing in the statute that would bar liability as a co-conspirator or an aider and abettor. For example, in United States v. Moran-Toala, 726 F.3d 334 (2d Cir. 2013), the Second Circuit vacated a conviction for conspiracy to violate the CFAA, but only because the district court had instructed the jury that it was permissible to render inconsistent verdicts. Id. at 342-43. However, the Court implicitly approved the application of conspiratorial liability against the defendant. Id. at 345 (remanding for retrial on the unlawful computer access conspiracy charge); see Mintz v. Mark Bartelstein & Assocs., Inc., 906 F. Supp. 2d 1017, 1029 (C.D. Cal. 2012) (granting summary judgment for defendants where Plaintiff failed to show sufficient loss, but Defendants did not contest violation of the CFAA where a defendant had instructed another person to access Plaintiff's email account). Moreover, the CFAA explicitly allows for liability under a conspiratorial theory of liability. 18 U.S.C. § 1030(b) (stating that "[w]hoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section"). Plaintiffs are at least alleging that by instructing Jiang to access Enargy's server and encrypt the PH Project files, Wang engaged in conduct, in concert with Jiang or with Jiang acting as Wang's agent, that violated the CFAA. Plaintiffs appear to have a reasonable likelihood of success of showing that Wang's conduct constituted "access" under the CFAA.

c) Wang Exceeded Authorized Access

The parties also dispute whether Wang's conduct could "exceed authorized access," which the CFAA defines as meaning "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). Courts have taken different views as to what constitutes exceeding authorized access. Compare United States v. Rodriguez, 628 F.3d 1258, 1263-64 (11th Cir. 2010), cert. denied 131 S. Ct. 2166 (2011) with WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 206 (4th Cir. 2012). In a recent decision, another judge in this district aptly summarized the distinction:

> Courts have generally adopted one of two positions when interpreting the CFAA. A narrow interpretation reflects a technological model of authorization, whereby the scope of authorized access is defined by the technologically implemented barriers that circumscribe that access. Thus if Company C maintains two secure servers, X and Y, and issues Employee E valid login credentials for Server X but not for Server Y, then Employee E has authorized access to Server X, but not to Server Y. Any data accessed by Employee E from Server X would be with authorization no matter how Employee E used that information. However, if Employee E used his/her Server X access to illicitly access Server Y, any data thus accessed on Server Y would be outside the scope of authorization.
>
> By contrast, a broader interpretation defines access in terms of agency or use. Thus wherever an employee breaches a duty or loyalty, or a contractual obligation, or otherwise acquires an interest adverse to the employer, their authorization to access information stored on an employer's computer terminates and all subsequent access is unauthorized/exceeds the scope of authorization, whether or not the access is still technologically enabled. Thus, using the example stated above, Employee E *would* exceed the scope of his/her authorized access if data accessed from Server X was used for some purpose that was prohibited by Employee E's contractual or legal obligations to Company C.

Advanced Micro Devices, Inc. v. Feldstein, --- F. Supp. 2d ----, No. 13-40007-TSH, 2013 WL 2666746, at *3 (D. Mass. June 10, 2013). The First Circuit has not taken a definitive position as to which theory of liability it has endorsed. As noted by the court in Feldstein, "[s]ome district judges have read EF Cultural Travel BV v. Explorica, Inc. (EF Cultural I), 274 F.3d 577 (1st

Cir. 2001) as an endorsement of the broader interpretation." Feldstein, 2013 WL 2666746, at *5 (citing Guest–Tek Interactive Entm't, Inc. v. Pullen, 665 F. Supp. 2d 42, 42 (D. Mass. 2009)). "Others have read EF Cultural I as supporting a broad interpretation only in dicta, and have adopted a narrower interpretation." Id. (citing Wentworth–Douglass Hosp. v. Young & Novis Prof'l Ass'n, 10-0120, 2012 WL 2522963 (D.N.H. Jun. 29, 2012)).

EF Cultural I affirmed the district court's grant of a preliminary injunction where the defendant, a travel company, used automatic "scraping" software to download price information from a competitor's website. EF Cultural I, 274 F.3d at 580. In doing so, the district court found that the plaintiff would likely prevail because the competitor was aided by a former employee of the plaintiff whose actions ran afoul of a confidentiality agreement that he had signed with the plaintiff. Id. at 583. In a later decision, the First Circuit clarified that:

> The panel [in EF Cultural I] held that the use of the scraper tool exceeded the defendants' authorized access to EF's website because (according to the district court's findings for the preliminary injunction) access was facilitated by use of confidential information obtained in violation of the broad confidentiality agreement signed by EF's former employees.

EF Cultural Travel BV v. Explorica (EF Cultural II), 318 F.3d 58, 61 (1st Cir. 2003). In other words, the First Circuit found that the defendant's actions exceeded authority under the CFAA because the defendants' access contravened a specific duty.

The Guest-Tek court held that an employee who had "full and unrestricted access to all of the information at issue" violated the CFAA where he "surreptitiously transposed thousands of Guest-Tek computer files onto his personal USB device and conspired with one of Guest-Tek's largest competitors to launch" a new company. Guest-Tek, 665 F. Supp. 2d at 43. In doing so, the court explicitly rejected a "narrow reading" of the CFAA, especially in light of recent "liberal" judicial interpretations of the statute. Id. at 45-46 (citing P.C. Yonkers, Inc. v.

Celebrations the Party and Seasonal Superstore, LLC, 428 F.3d 504, 510 (3rd Cir. 2005) (noting that "[e]mployers . . . are increasingly taking advantage of the CFAA's civil remedies to sue former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system")).

Wentworth-Douglass endorsed a narrow interpretation of "exceeding authorized access." In that case, the court ruled that a doctor who used his own password to access a computer system in a way proscribed by policy, but not blocked technically, did not violate the CFAA. Wentworth-Douglass, 2012 WL 2522963 at *4. The Court dismissed the suggestions of EF Cultural I and EF Cultural II that a broader interpretation of the CFAA should apply as dicta, finding that exceeding authorized access means "to obtain information . . . beyond that which he was entitled to obtain." Id. (quoting Nucor Steel Marion, Inc. v. Mauer, No. 10-207, 2010 WL 5092774 (D.N.H. Dec. 7, 2010)).

Feldstein squares these approaches, noting that in EF Cultural I, the defendant "gave unique information to a competitor that allowed that competitor to log into the employer's website as a tour leader and obtain sensitive pricing information to which the competitor would otherwise not have had access," Feldstein, 2013 WL 2666746, at *5, which demonstrates that the defendant exceeded his authorization because it "involves gaining information through a means of deception" that involved some level of fraudulent intent to exceed authorization. Id.[1]

Applying this standard to the instant case and mindful of the element of the claim that the a defendant knowingly and with intent to defraud accessed a computer, the key issue is whether

[1] Case law interpreting the Stored Communications Act, 18 U.S.C. § 2701, and analyzing "exceeding the scope of authorization" in terms of agency and use further supports this interpretation. See, e.g., Cheng v. Romo, No. 11-10007-DJC, 2012 WL 6021369, at *4 (D. Mass. Nov. 28, 2012); Clements-Jeffrey v. City of Springfield, Ohio, 810 F. Supp. 2d 857, 878 (S.D. Ohio 2011).

Wang's alleged access here exceeded his authority to access Enargy's server. Plaintiffs' affidavits demonstrate that "the only persons authorized to copy, download, encrypt and delete confidential technology files were the two (2) network administrators and the general manager of Enargy China." D. 8-1 ¶ 10. Defendants have not disputed this contention and Wang does not fall into either category. Id. ¶ 6. In addition, Wang's actions employed an element of deception in that he acted without his employer's consent or knowledge, see id. ¶ 10, and using his assistant as a conduit, who had every reason to trust that Wang was acting within the scope of his authorization, when in fact, Wang incorrectly misled Jiang by telling him that encryption was "necessary." D. 8-2. ¶ 11. The Court therefore finds that Wang's conduct employed a "means of a deception," Feldstein, 2013 WL 2666746, at *5, and therefore exceeded the scope of his authorization.

Defendants contended at oral argument that Wang could not have exceeded his authorized access by restricting the use of the PH Project files on Enargy's server. They argued that it was Wang's understanding that the files would remain his property and, therefore, encrypting the files was merely an exercise of his ownership rights. Although there appears to be a dispute between the parties of the ultimate ownership over the PH Project files, the record presently before the Court evidences that Wang and Enargy were collaborating on the PH Project and the development of the project files. Wang worked for the research and development "department," "le[ading] the design and development" of the PH Project, suggesting that there was a department or team in place working on the project. D. 8-1 ¶¶ 6-7. He was an employee of the company and not an outside contractor. Id.; D. 17-1 ¶ 23. Wang attests that he "had senior authority to examine and approve every engineering plan," suggesting that he did not personally create every plan. D. 17-1 ¶ 23. Communications between Wang, Jacky Chen and

Liu further corroborate the collaborative efforts to sell the product to Sichuan Chengye. D. 19-2. That is, even as Wang contends that he owns the files, there is credible evidence that Enargy had at least some ownership right in the PH Project files. By restricting access to only himself, however, Wang negated the ongoing collaboration, an action that strongly supports Plaintiffs' contention that Wang exceeded his authorized access, contrary to Defendants' assertions.

Moreover, even if Wang was the sole owner of the PH Project files and their underlying intellectual property, Wang's conduct still interfered with the use of Enargy's server. Enargy has been unable to access the PH Project files and continue the research and development of this project. D. 8-2 ¶ 20. Despite "tremendous efforts and significant expense" by Enargy's internal IT staff and outside experts, Enargy has not been able to access these locked files on its own server. Id. The parties have not cited and the Court is not aware of any published case in which a defendant was found liable or not liable for encrypting files on a company's server, thereby restricting access only to that defendant. However, other courts have found that "unauthorized interference, intermeddling, and access with [a company], its website, computer systems, and its servers" is actionable both under the common law and under the CFAA. Craigslist Inc. v. 3Taps Inc., --- F. Supp. 2d ----, No. 12-03816, 2013 WL 1819999, at *5, 15 (N.D. Cal. Apr. 30, 2013) (denying motion to dismiss trespass claim but also holding that conduct stated plausible CFAA claim); see also United States v. Fowler, 445 Fed. App'x 298, 300 (11th Cir. 2011) (finding sufficient evidence to support CFAA conviction where defendant's "interference with the computer system" "interrupted employees' ability to access" company data); United States v. Mitra, 405 F.3d 492, 494-96 (7th Cir. 2005) (affirming CFAA conviction under CFAA where defendant interfered with a municipality's use of a computer-based radio system for police, fire, ambulance and other emergency communications); Facebook, Inc. v. Power Ventures, Inc., 844

F.Supp.2d 1025, 1038–39 (N.D. Cal. 2012) (holding that access was without authorization under the CFAA where defendants "circumvented technical . . . barriers in place to restrict or bar a user's access").

Further, the Court finds that logically, liability should extend to the instant facts. For instance, consider hypothetically, if the PH Project files were tangible goods and that Wang had locked the files in his file cabinet (owned by the company) before leaving Enargy and took the key, refused to return it and Enargy's efforts to pick the lock were wholly unsuccessful. Surely such conduct would create a civil remedy for plaintiffs under a conversion theory. See Evergreen Marine Corp. v. Six Consignments of Frozen Scallops, 4 F.3d 90, 98 (1st Cir. 1993) (finding that plaintiff, who retained reclamation rights to goods, could state common law claim for conversion against the defendant who refused to return goods to plaintiff). Similarly here, Wang's actions to restrict effectively the use of Enargy's virtual file cabinet run afoul of the CFAA and, on the record presently before the Court, suggest that Enargy has a likelihood of success of showing that Wang knowingly and with intent to defraud accessed Enargy's server and such access (for the purpose of locking and encrypting Enargy's future access to the project files) exceeded his authority for such access.[2]

d) The Computer Fraud and Abuse Act Applies to Conduct Affecting Computers Outside the United States

During oral argument, counsel for Defendants contended that the CFAA does not apply to the conduct of defendants in the United States who access computers outside the United States. Although the crux of Plaintiffs' allegations are that Wang instructed Jiang to access a computer in China, not in the United States, D. 8-2 ¶ 11, the Court rejects Defendants'

[2] The parties do not seriously contest that Wang took something "of value" (i.e., copy of the project files and then barred Enargy's access to those files on the server), but the Court concludes that this element has been shown here as well.

contention. As an initial matter, the term "protected computer" is defined by the CFAA as "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States[.]" 18 U.S.C. § 1030(e)(2). Consequently, courts have found that defendants violate the CFAA even where they access computers outside the United States. Four Seasons Hotels & Resorts B.V. v. Consorcio Barr, S.A., 267 F. Supp. 2d 1268, 1322 (S.D. Fla. 2003) (finding that defendant violated CFAA by through "intentional attempts to access remote computers within the Four Seasons' protected network [where such access] involved actual access of the Four Seasons OpenReach VPN device in Caracas[, Venezuela]"), aff'd in part, rev'd in part sub nom. Four Seasons Hotels v. Consorcio Barr S.A., 138 Fed. App'x 297 (11th Cir. 2005). Similarly, courts have found that conduct outside the United States can form the basis for CFAA liability. See United States v. Ivanov, 175 F. Supp. 2d 367, 370-71 (D. Conn. 2001) (denying motion to dismiss CFAA count where defendant, although physically located in Russia, accessed computer located within United States).

For all of these reasons, the Court finds that Plaintiffs are likely to succeed on the merits of their CFAA claim.

2. Plaintiffs Have Demonstrated a Likelihood of Success on Their Conversion Claim

Plaintiffs seek injunctive relief barring Chen from interfering with the bank account owned by Enargy's Massachusetts entity. The claim that Plaintiffs tie to the relief sought is Plaintiffs' conversion claim. "A plaintiff asserting a conversion claim under Massachusetts law must show that: (1) the defendant intentionally and wrongfully exercised control or dominion over the personal property; (2) the plaintiff had an ownership or possessory interest in the

property at the time of the alleged conversion; (3) the plaintiff was damaged by the defendant's conduct; and (4) if the defendant legitimately acquired possession of the property under a good-faith claim of right, the plaintiff's demand for its return was refused. Evergreen Marine Corp., 4 F.3d at 95.

At oral argument, Defendants conceded that the bank account in question is registered in Enargy's name. They further conceded that Chen is no longer employed by Enargy. Accordingly, any further interference with the bank account would be a wrongful exercise of control over the Plaintiffs' property. Enargy has also shown that Chen had appropriated Enargy's bank account as her personal bank account and that, at the time of her actions, Plaintiffs had an ownership interest in the account. D. 8-13 at 2; D. 8-15. In having been deprived the sole use of their property, Plaintiffs have been damaged. Finally, when Plaintiffs inquired as to Chen's continued interference of the bank account, Chen continued to assert that the account belonged to her. Id. Accordingly, Plaintiffs have demonstrated that they are likely to succeed on their conversion claim.

3. Plaintiffs Have Not Shown a Substantial Likelihood of Success on Their Misappropriation of Trade Secrets Claim

a) Choice of Law

Defendants have raised a choice of law issue that the Court must address before determining likelihood of success on the merits of Plaintiffs' trade secrets claim. Defendants contend that Chinese law applies to this case because China has the most significant relationship to the parties. D. 17 at 8. "A federal court sitting in diversity must apply the choice of law principles of the forum state," and thus, this court "must look to Massachusetts choice of law rules." Dunfey v. Roger Williams Univ., 824 F. Supp. 18, 20 (D. Mass. 1993). When faced with a tort claim, the Massachusetts Supreme Judicial Court applies the Restatement of Conflict of

Laws' "functional approach" examining which state has the "most significant relationship" to the occurrence and the parties. Cosme v. Whitin Mach. Works, Inc., 417 Mass. 643, 646 (1994). When evaluating this relationship, courts look to: (a) the place where the injury occurred; (b) the place where the conduct causing the injury occurred; (c) the domicile, residence, nationality, place of incorporation and place of business of the parties; and (d) the place where the relationship, if any, between the parties is centered. Id. at 647 (citing Rest. 2d Conflict of Laws § 145).

Here, the injury occurred in China, from where the PH project files were allegedly stolen. D. 8-2 ¶ 15. The conduct occurred in Massachusetts because that is the location from where Wang called Jiang to transmit the PH project files. Id. ¶ 11. The parties are roughly equally split between Massachusetts and China. Both Defendants, Enargy Mass. and Zoomkoh Management LLC being Massachusetts citizens, while Enargy China and Jacky Chen are Chinese citizens. D. 1 ¶¶ 1-6. The dispositive factor, then, is where the relationship between the parties is centered. Here, Enargy China incorporated a Massachusetts entity with the purpose of developing operations in Massachusetts under Wang's supervision. D. 1 ¶ 18. This plan never came to fruition, however, with Wang taking trips of up to 180 days to China to work on Enargy's design and development efforts. D. 17-1 ¶ 23. On the record presently before the Court, the factors weigh slightly in favor of applying Chinese law to this dispute. Plaintiffs have not demonstrated the relevant Chinese law to apply to their misappropriation of trade secrets claims or the likelihood of success under such law. Thus, they have not met their burden here. Esso Standard Oil Co. (Puerto Rico) v. Monroig-Zayas, 445 F.3d 13, 18 (1st Cir. 2006) (noting that "[t]he party seeking the preliminary injunction bears the burden of establishing [likelihood of success on the merits]").

b) Even Assuming Massachusetts Law Applies, Plaintiffs Have Not Demonstrated a Substantial Likelihood of Success

Even assuming that Massachusetts law applied, as the Plaintiffs contend it does, Plaintiffs have not yet demonstrated that they are likely to succeed on their misappropriation of trade secrets claim. To prevail on a misappropriation of trade secrets claim under Massachusetts law, a plaintiff must demonstrate that (1) "the information at issue must constitute a trade secret, (2) the plaintiff must have taken reasonable steps to secure the confidentiality of the trade secret, and (3) the defendant must have used improper means to obtain the trade secret." Optos, Inc. v. Topcon Med. Sys., Inc., 777 F. Supp. 2d 217, 238 (D. Mass. 2011). Courts also recognize that for a defendant to be liable for misappropriation of trade secrets, the trade secrets must, in fact, belong to the plaintiff. See, e.g., Curtiss-Wright Corp. v. Edel-Brown Tool & Die Co., Inc., 381 Mass. 1, 3 n. 2 (1980).

Here, there is a significant factual dispute as to who owns the trade secrets in question. Enargy asserts that they belong to the company, D. 8-1 ¶ 8, while Wang asserts that they always remained his property. D. 17-1 ¶¶ 38, 40. The parties have acknowledged that there is no formal agreement governing their relationship, which the Court might look to for guidance. Id. ¶ 41. In light of this factual dispute and on this record, the Court cannot say that Plaintiffs have demonstrated a "substantial likelihood" of success on their trade secrets claim. Nieves-Marquez, 353 F.3d at 120.

4. Plaintiffs Have Not Demonstrated a Substantial Likelihood of Success on Their Breach of Fiduciary Duty Claim

Plaintiffs allege that Wang, as a senior executive and director of Enargy's research and development department, had a fiduciary duty to the company and breached it by "misappropriating and wrongful[ly] using the [project files and trade secrets]." D. 1 at ¶¶ 107-

10. An essential element of a breach of a fiduciary duty claim is the existence of a fiduciary duty. "Under Massachusetts law, officers and directors owe a fiduciary duty to protect the interests of the corporation they serve." Geller v. Allied-Lyons PLC, 42 Mass. App. Ct. 120, 122 (1997). Senior executives are considered to be corporate fiduciaries and to owe their company a duty of loyalty. Id. (assuming that senior vice president owed fiduciary duty) (citing Chelsea Indus. v. Gaffney, 389 Mass. 1, 11-12 (1983)). Partners also owe fiduciary duties to other partners. Meehan v. Shaughnessy, 404 Mass. 419, 433 (1989). At oral argument, Plaintiffs disclaimed the notion that Wang was a "partner" of Enargy. Plaintiffs have not alleged that Wang was a director of Enargy. Finally, the record is unclear as to whether Wang was of sufficient rank at Enargy to be considered a "senior executive." See Chelsea, 389 Mass. at 11-12.

Certainly, mere employees can breach fiduciary duties to their employers under certain circumstances. Massachusetts courts have construed an employees' misappropriation of their employers' trade secrets as a breach of fiduciary duty. See Intertek Testing Servs. NA, Inc. v. Curtis-Strauss LLC, No. 98903, 2000 WL 1473126, at *9 (Mass. Super. Aug. 8, 2000) (quoting Augat, Inc. v. Aegis, Inc., 409 Mass. 165, 172-73 (1991)). However, as alleged in the complaint, the claim of breach of fiduciary duty rises and falls with Plaintiffs' misappropriation of trade secrets claim. As discussed above, Plaintiffs have not demonstrated a substantial likelihood of success on their claim for misappropriation of trade secrets. Accordingly, the Court finds that Plaintiffs have not demonstrated same, on the present record, in regard to their claim for breach of fiduciary duty against Wang.

B. Plaintiffs Have Demonstrated the Risk of Irreparable Harm Absent Injunctive Relief

As a general matter, where "plaintiffs can show a likelihood of success on the merits, irreparable harm is usually presumed . . . [a]n exception exists when plaintiffs are aware (or have reason to be aware) of the [alleged conduct], and do not bring suit. Fritz v. Arthur D. Little, Inc., 944 F. Supp. 95, 98 (D. Mass. 1996) (citing Concrete Machinery Co. v. Classic Lawn Ornaments, 943 F.2d 600, 611 (1st Cir. 1988); Bourne Co. v. Tower Records, Inc., 976 F.2d 99, 101 (2d Cir. 1992)). Here, Plaintiffs waited some time before filing this lawsuit. The court therefore engages in a fulsome analysis of Plaintiffs' alleged irreparable harm.

Plaintiffs seek a three-pronged injunction. First, they ask the Court to return all copies of the PH and Five Series files Wang possesses or controls. D. 8 at 1. This injunctive relief necessarily flows from a demonstration that Plaintiffs can demonstrate likelihood of success on the merits of their misappropriation of trade secrets claim. See Touchpoint Solutions, Inc. v. Eastman Kodak Co., 345 F. Supp. 2d 23, 32 (D. Mass. 2004). As the Court has been unable to conclude the likelihood of Plaintiffs' success on this claim, the Court dispenses with the analysis of whether Plaintiffs will suffer irreparable harm absent a return of the PH Project files.

Second, Plaintiffs ask the Court to order Wang to disclose the password for the PH project files located on Enargy's server. D. 8 at 1. This relief is aimed at curbing irreparable harm flowing from Wang's conduct that the Court has found violates the CFAA. In essence, Plaintiffs assert that Wang's conduct has prevented Enargy from enjoying the uninterrupted use of its property. Analogizing this harm to the use of tangible personal property, courts have found that such interference constitutes irreparable harm. Proulx v. Basbanes, 354 Mass. 559, 560-62 (1968) (enjoining laundry business from operating business where noise and vibrations caused by defendant caused mortar to fall from the plaintiffs' cellar, cracks to appear in the foundation

and windows to loosen from their frames). Furthermore, Plaintiffs' inability to make use of the PH Project files has hampered Enargy from further developing the product resulting in the loss of goodwill, D. 8-1 ¶¶ 16-17, which can also form the basis for irreparable harm. Ross-Simons of Warwick, Inc. v. Baccarat, Inc., 102 F.3d 12, 20 (1st Cir. 1996). Finally, civil violations of the CFAA can provide the basis for injunctive relief. EF Cultural I, 274 F.3d at 578-79. Thus, Plaintiffs have shown the likelihood of irreparable harm in the absence of granting this form of equitable relief.

Third, they ask the Court to enjoin Defendants from interfering with Enargy's bank account. D. 8 at 1. For reasons explained above, interference with a possessory interest in personal property can constitute irreparable harm and does here in the absence of any legitimate remaining interest that Chen, no longer employed by Enargy, could assert in the property. Accordingly, the Court finds that Plaintiffs will suffer irreparable harm absent an injunction prohibiting Defendants from interfering with Enargy's bank account.

C. The Public Interest Favors Injunctive Relief

It is in the public interest to protect and create incentives for innovation. See Amgen, Inc. v. F. Hoffman-LaRoche, Ltd., 581 F. Supp. 2d 160, 210 (D. Mass. 2008), rev'd in part on other grounds 580 F.3d 1340 (1st Cir. 2009). The record indicates that significant time, effort, and capital were invested by Enargy in the PH and Five Series projects. D. 8-1 ¶ 24. Failure to award injunctive relief, at least in the respects that the Court shall grant, in this case thus fails to protect and reward innovation.

D. The Balance of Harms Tips Slightly in Enargy's Favor

A court "must balance the relevant harms before granting injunctive relief." Maine People's Alliance And Natural Res. Def. Council v. Mallinckrodt, Inc., 471 F.3d 277, 296 (1st

Cir. 2006). The Court declines to order Wang to return copies of the files he possesses, which would prevent Wang from working on the PH Project even with Sichuan Chengye, and in light of the ownership dispute discussed supra, such an order may cause Wang undue harm.

However, to order Wang to disclose the password for those files encrypted on Enargy's server allows both parties to continue to work on the projects while the parties litigate the ownership of the trade secrets. In other words, as the purpose of a preliminary injunction is to preserve the status quo, the most appropriate way to do so in this case is to allow both parties to have access to the project files during the pendency of the litigation. CMM Cable Rep., Inc. v. Ocean Coast Properties, Inc., 48 F.3d 618, 620 (1st Cir. 1995) (noting that "[t]he purpose of a preliminary injunction is to preserve the status quo, freezing an existing situation so as to permit the trial court, upon full adjudication of the case's merits, more effectively to remedy discerned wrongs"). In light of significant evidence in the record at least of joint ownership of these files, D. 8-1 ¶¶ 6-7; D. 17 ¶ 23 (demonstrating collaboration between Wang and Enargy), the Court cannot say that the harm Wang faces by disclosing the password is outweighed by Enargy's legitimate interest in unfettered access to its server and the ability to compete with Wang during the pendency of the dispute.

As to an order prohibiting Defendants' continued use of Enargy's bank account, as Defendants concede that they no longer have any rights in the account, the balance of harms weighs heavily in Plaintiffs' favor.

E. Plaintiffs Have Not Met Their Burden for the Motion to Attach

The parties agree that attachment of real property is governed by state law, namely Massachusetts Rule of Civil Procedure 4.1, which provides that a court may order attachment "upon a finding by the court that there is a reasonable likelihood that the plaintiff will recover

judgment, including interest and costs, in an amount equal to or greater than the amount of the attachment over and above any liability insurance shown by the defendant to be available to satisfy the judgment."

Although the Court has found a likelihood of success on the CFAA claim, Plaintiffs have not made the requisite showing as to the amount of that recovery, nor have they offered any evidence of Defendants' liability insurance or lack thereof. Accordingly, the court DENIES the motion to attach without prejudice.

V. Conclusion

For the above reasons, the Court ALLOWS IN PART the motion for a preliminary injunction (pending the posting of a bond of $10,000 under Fed. R. Civ. P. 65(c)), D. 7, to the extent that the Court ORDERS: (1) Wang to disclose the password for the encrypted PH Project files located on Enargy's server; and (2) Defendants to cease the use of any bank account registered in the name of Enargy Corporation, including but not limited to Bank of America Acct. No. XXXXXXXX9064. Plaintiffs' motion to attach, D. 9, is DENIED without prejudice.

So Ordered.

/s/ Denise J. Casper
United States District Judge